CLAIMS

What is claimed is:

1. A programmable apparatus for authenticating and authorizing a service request sent from a service client to a service provider, comprising:

a processor;

a memory;

an authorization database in the memory;

a service request filter program in the memory directing the processor to

receive an incoming service request from the service client on a communication channel, the service request having a digital certificate attached;

extract a service client identifier from the digital certificate associated with the service request;

store the service client identifier in the memory; and

send the service request on the communication channel to a web service manager;

a service client authentication program in the memory directing the processor to

responsive to receiving an authentication request from a web service manager, match the service client identifier with a service client record in the authorization database having the same service client identifier; and

responsive to matching the service client identifier with a record in the authorization database, call a service authorization program in the memory;

wherein the service authorization program directs the processor to

determine if the service client identifier associated with the service request is authorized to access the service provider; and

responsive to determining that the service request is authorized, authorize the service provider to process the request.

2. The programmable apparatus of claim 1 wherein the service request filter program further directs the processor to authenticate the digital certificate with the issuing certification authority.

3. The programmable apparatus of claim 1 wherein the digital certificate is an X.509 digital certificate.

4. The programmable apparatus of claim 1 wherein the service client identifier is a Distinguished Name.

5. The programmable apparatus of claim 1 wherein the digital certificate is self-signed.

6. The programmable apparatus of claim 1 further comprising an authorization log.

7. The programmable apparatus of claim 6 wherein the service client authentication program further records the service client identifier in the authorization log.

8. The programmable apparatus of claim 6 wherein the service authorization program further records the service client identifier and service request in the authorization log.

9. A web service architecture having the programmable apparatus of claim 1.

10. A computer-readable memory for causing a computer to authenticate and authorize service requests sent from a service client to a service provider, comprising:

a computer-readable storage medium;

an authorization database stored in the storage medium;

a service request filter program stored in the storage medium, wherein the storage medium, so configured by the service request filter program, causes the computer to

receive an incoming service request on a communication channel, the service request having a digital certificate attached;

extract a service client identifier from the digital certificate associated with the service request;

store the service client identifier in the memory; and

send the service request on the communication channel to a web service manager;

a service client authentication program stored in the storage medium, wherein the storage medium, so configured by the service client authentication program, causes the computer to

responsive to receiving an authentication request from a web service manager, match the service client identifier with a service client record in the authorization database having the same service client identifier; and

responsive to matching the service client identifier with a record in the authorization database, call a service authorization program in the memory;

wherein the service authorization program is stored in the storage medium, and the storage medium, so configured by the service authorization program, causes the computer to

determine if the service client identifier associated with the service request is authorized to access the service provider; and

responsive to determining that the service request is authorized, authorize the service provider to process the request.

11. The computer readable memory of claim 10 wherein the service request filter program further causes the computer to authenticate the digital certificate with the issuing certification authority.

12. The computer-readable memory of claim10 wherein the digital certificate is an X.509 digital certificate.

13. The computer-readable memory of claim10 wherein the service client identifier is a Distinguished Name.

14. The computer-readable memory of claim 10 wherein the digital certificate is self-signed.

15. The computer-readable memory of claim 10 further comprising an authorization log.

16. The computer-readable memory of claim 15 wherein the service client authentication program further causes to the computer to record the service client identifier in the authorization log.

17. The computer-readable memory of claim 15 wherein the service authorization program further causes the computer to record the service client identifier and service request in the authorization log.

18. A method of authenticating and authorizing a service request sent from a service client to a service provider, comprising the steps of:

receiving an incoming service request on a communication channel, the service request having a digital certificate attached;

extracting a service client identifier from the digital certificate associated with the service request;

storing the service client identifier in the memory;

sending the service request to a web service manager;

responsive to receiving an authentication request from a web service manager, matching the service client identifier with a service client record in the authorization database having the same service client identifier;

determining if the service client identifier associated with the service request is authorized to access the service provider; and

responsive to determining that the service request is authorized, authorizing the service provider to process the request.

19. The method of claim 18 further comprising the step of authenticating the digital certificate with the issuing certification authority.

20. The method of claim 18 wherein the digital certificate is an X.509 digital certificate.

21. The method of claim 18 wherein the service client identifier is a Distinguished Name.

22. The method of claim 18 wherein the digital certificate is self-signed.

23. The method of claim 18 further comprising the step of recording the service client identifier in an authorization log.

24. The method of claim 18 further comprising the step of recording the service client identifier and service request in the authorization log.